

PCT/JP 2004/011630

REC'D 26 AUG 2004

WIPO

06.08.2004

日 本 国 特 許
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 8 月 7 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 2 8 8 7 9 4
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 2 8 8 7 9 4]

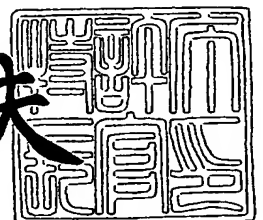
出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 4 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office.

今 井 康 夫



出 証 番 号 出 証 特 2 0 0 4 - 3 0 3 1 4 3 6

【書類名】 特許願
【整理番号】 2030750084
【提出日】 平成15年 8月 7日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 15/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 田磨 雅基
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 井上 和紀
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 伊藤 快
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100099254
 【弁理士】
 【氏名又は名称】 役 昌明
【選任した代理人】
 【識別番号】 100100918
 【弁理士】
 【氏名又は名称】 大橋 公治
【選任した代理人】
 【識別番号】 100105485
 【弁理士】
 【氏名又は名称】 平野 雅典
【選任した代理人】
 【識別番号】 100108729
 【弁理士】
 【氏名又は名称】 林 紘樹
【手数料の表示】
 【予納台帳番号】 037419
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9102150
 【包括委任状番号】 9116348
 【包括委任状番号】 9600935
 【包括委任状番号】 9700485

【書類名】 特許請求の範囲**【請求項 1】**

メモリ領域内にセキュリティレベルが異なる複数の分割領域を有する情報記憶装置であって、

前記分割領域のメモリ領域内でのアドレスを管理する領域管理手段と、

前記分割領域の数または大きさを更新する際の更新条件を管理する領域更新条件管理手段と、

前記分割領域の数または大きさの更新を要求する分割要求が前記更新条件を満足するか否かを判断する領域更新判断手段と、

前記分割要求が前記更新条件を満足するとき、前記分割要求に従ってメモリ領域内の分割領域の更新を実行する領域更新手段と

を備えることを特徴とする情報記憶装置。

【請求項 2】

前記更新条件として、更新の手続きに関する手続条件と、更新の内容に関する実体条件とが規定されていることを特徴とする請求項 1 に記載の情報記憶装置。

【請求項 3】

前記実体条件として、少なくとも更新可能回数、分割領域の最大数、分割領域の最大サイズのいずれかが規定されていることを特徴とする請求項 2 に記載の情報記憶装置。

【請求項 4】

前記領域更新手段は、前記分割要求に従ってメモリ領域内の実データが記録されていない未使用領域を再分割することを特徴とする請求項 1 に記載の情報記憶装置。

【請求項 5】

前記分割領域の更新が正常に行われたことを示すレシートを作成するレシート作成手段を備えることを特徴とする請求項 1 に記載の情報記憶装置。

【請求項 6】

前記レシートには、更新後における分割領域のサイズ、または更新前後の分割領域の差分サイズが記述されていることを特徴とする請求項 5 に記載の情報記憶装置。

【請求項 7】

前記領域更新手段が実行するメモリ領域内の分割領域の更新に関する情報を出力する出力手段と、前記情報に対するユーザの確認登録を受け付ける受付手段とを備え、前記分割領域の更新は、確認登録の受付により始めて実効性を持つことを特徴とする請求項 1 に記載の情報記憶装置。

【書類名】 明細書**【発明の名称】** メモリ領域に分割領域を持つ情報記憶装置**【技術分野】****【0001】**

本発明は、メモリ領域を備える半導体メモリカードやICカード等の情報記憶装置に関する。

【背景技術】**【0002】**

近年、一枚のカード上にセキュリティ強度やアクセス手法を異にする複数の領域を備えた半導体メモリカードが開発されている。例えば下記特許文献1には、記憶領域として、認証した機器だけがアクセスできる認証領域と、認証を必要とせずにアクセスできる非認証領域とを持つ半導体メモリカードが開示されている。

このメモリカードは、図8に示すように、記憶領域を構成するフラッシュメモリ303のICチップと、記憶領域への書き込み・読み出しを制御するコントロールIC302とを内蔵し、フラッシュメモリ303は、正当な機器であると認証することができた機器だけに対してアクセスを許可する認証領域332と、そのような認証を必要とすることなくアクセスを許可する非認証領域331とを備えている。

また、コントロールIC302は、このメモリカード109にアクセスしようとする相手機器の正当性を認証する認証部321と、コマンドピンを介して入力されたコマンドの種類を判定し、その種類に応じて各種構成要素を制御するコマンド判定制御部322と、フラッシュメモリ303の認証領域332へのデータ書き込み及び読み出しを実行する認証領域アクセス制御部325と、非認証領域331へのデータ書き込み及び読み出しを実行する非認証領域アクセス制御部326とを備えている。

【0003】

このメモリカード109の認証領域332にアクセスする端末は、メモリカード109の認証部321と認証を行い、認証に成功すると、認証領域アクセス制御部325を通じて、認証領域332へのデータの書き込みや読み出しが可能になる。また、非認証領域331へのデータの書き込み・読み出しは、非認証領域アクセス制御部326を通じて自由に行うことができる。

【0004】

このメモリカード109の非認証領域331及び認証領域332は、フラッシュメモリ303上の一定のアドレスを境界として区分されており、境界アドレスを変更して各領域の大きさを可変することができる。領域を変更する場合は、メモリカード109にアクセスする装置が、メモリカード109との認証を行った後、領域変更の専用コマンドで非認証領域331の大きさをメモリカード109に送る。メモリカード109は、その領域変更コマンドを受け取ると、その値をメモリカード109内の不揮発な作業領域に保存し、以降のアクセスにおいては、その値を新たな境界アドレスとして、認証領域332及び非認証領域331へのアクセス制御を実行する。

【特許文献1】 特開2001-14441号公報

【発明の開示】**【発明が解決しようとする課題】****【0005】**

しかし、このように複数の分割された領域を持つ従来の情報記憶装置は、ユーザに交付する段階で、既に、カード発行者の意向に基づいてメモリ領域が分割されている。そのため情報記憶装置の利用形態が個々のユーザによって違っていても、各ユーザは、お仕着せの分割領域を持つ情報記憶装置しか入手することができない。

【0006】

本発明は、こうした従来の問題点を解決するものであり、メモリ領域を分割する分割領域の数や大きさを、ユーザの意向に基づいて設定することができる情報記憶装置を提供することを目的としている。

【課題を解決するための手段】**【0007】**

本発明では、メモリ領域内にセキュリティレベルが異なる複数の分割領域を有する情報記憶装置に、分割領域のメモリ領域内でのアドレスを管理する領域管理手段と、分割領域の数または大きさを更新する際の更新条件を管理する領域更新条件管理手段と、分割領域の数または大きさの更新を要求する分割要求が更新条件を満足するか否かを判断する領域更新判断手段と、分割要求が更新条件を満足するとき、分割要求に従ってメモリ領域内の分割領域の更新を実行する領域更新手段とを設けている。

この情報記憶装置は、ユーザの意向を反映した分割要求により、メモリ領域内の分割領域が更新される。

【0008】

また、本発明の情報記憶装置では、更新条件として、更新の手続きに関する手続条件と、更新の内容に関する実体条件とが規定されている。

そのため、分割要求が手続条件及び実体条件を満たすならば、ユーザが情報記憶装置の交付を受けるときに、そのメモリ領域は、分割要求に基づいてユーザの意向に沿って分割され、また、交付を受けた後の使用した情報記憶装置のメモリ領域は、分割要求に基づいて再分割される。

【0009】

また、本発明の情報記憶装置では、実体条件として、少なくとも更新可能回数、分割領域の最大数、分割領域の最大サイズのいずれかが規定されている。

そのため、更新回数が実体条件で規定された回数以内であり、あるいは、分割領域の数やサイズが規定値以内であれば、分割領域の更新は可能である。

【0010】

また、本発明の情報記憶装置では、領域更新手段が、分割要求に従ってメモリ領域内の実データが記録されていない未使用領域を再分割する。

そのため、分割領域が更新されても、既に記録された実データは保存される。

【0011】

また、本発明の情報記憶装置では、分割領域の更新が正常に行われたことを示すレシートを作成するレシート作成手段を設けている。

また、このレシートには、更新後における分割領域のサイズ、または更新前後の分割領域の差分サイズを記述している。

このレシートを見ることにより、分割領域の更新結果を知ることができる。

【0012】

また、本発明の情報記憶装置では、領域更新手段が実行するメモリ領域内の分割領域の更新に関する情報を出力する出力手段と、前記情報に対するユーザの確認登録を受け付ける受付手段とを設け、分割領域の更新は、確認登録の受付により始めて実効性を持つようにしている。

そのため、ユーザは、カードメーカーに事前に情報記憶装置の分割要求について伝え、この要求に従って領域分割された情報記憶装置を店頭等で受け取るときに、情報記憶装置にパスワードを登録して、情報記憶装置を使用可能な状態にする、といった運用を行うことができる。

【発明の効果】**【0013】**

本発明の情報記録装置は、メモリ領域を分割する分割領域の更新条件を保持し、分割要求が更新条件を満たす場合に、その要求に従って分割領域を更新するように構成しているため、メモリ領域にユーザの意図する分割領域を設定して交付することができ、また、交付後の情報記録装置のメモリ領域をユーザの意向に沿って再設定することができる。

【発明を実施するための最良の形態】**【0014】**

本発明の実施形態では、ユーザの意向に基づいて大きさを設定する領域として、認証領

域、非認証領域及びセキュア領域の三領域を有する情報記憶装置について説明する。

認証領域、非認証領域及びセキュア領域を有する情報記憶装置（ここでは「セキュアメモリカード」と呼ぶことにする）は、最近、出願人が開発したカードであり、図7のブロック図に示すように、大別して、制御部20と、フラッシュメモリから成る大容量不揮発性メモリ50と、耐タンパー性のIC部11とを備えている。

【0015】

大容量不揮発性メモリ50は、認証した機器だけがアクセスできる認証領域52と、認証を必要とせずにアクセスできる非認証領域53と、IC部11のみがアクセスできるセキュア領域51と、これらの領域のアドレス情報が格納されたアドレス情報管理領域54とを有している。

制御部20は、R/W装置69との間でデータの授受を行うデータI/F部21と、R/W装置69との間でコマンドの授受を行うコマンドI/F部22と、R/W装置69を認証する制御認証部23と、受け付けたコマンドを解釈してコマンドに応じた処理を行う制御コマンド処理部24と、大容量不揮発性メモリ50へのアクセスを制御するとともにIC部11とのデータの受け渡し窓口となるアクセス制御部25と、大容量不揮発性メモリ50との間でデータを受け渡す大容量不揮発性メモリI/F部26とを備えている。

【0016】

また、IC部11は、内部不揮発性メモリ41と、制御部20との間でデータやコマンドの授受を行うI/F部12と、コマンドを解釈してコマンドに応じた処理を行うICコマンド処理部13と、内部不揮発性メモリ41及びセキュア領域51にファイル形式で格納されたデータを管理するファイル管理部14と、R/W装置69を認証し、認証したR/W装置69に対して内部不揮発性メモリ41及びセキュア領域51へのデータアクセスを許可するIC認証部15と、内部不揮発性メモリ41及びセキュア領域51への書き込み/読み出しデータに対して内部不揮発性メモリ41に格納された鍵を用いて暗号化/復号化を行う暗復号回路17と、内部不揮発性メモリ41及びセキュア領域51の管理を行うメモリ管理部16と、内部不揮発性メモリ41へのデータの授受を行う内部不揮発性メモリI/F部18とを備えている。

【0017】

このセキュアメモリカード10の非認証領域53へのデータの書き込み・読み出しを行うR/W装置69は、非認証領域53へのアクセスを要求するコマンドをセキュアメモリカード10に送信する。制御コマンド処理部24は、そのコマンドを解釈して、アクセス制御部25に大容量不揮発性メモリ50へのアクセス制御を指示し、R/W装置69からデータI/F部21を通じて送られたデータが非認証領域53に書き込まれ、また、非認証領域53から読み出されたデータがデータI/F部21を介してR/W装置69に送信される。

【0018】

また、認証領域52へのデータの書き込み・読み出しを行うR/W装置69は、認証を要求するコマンドを送信して制御認証部23との間で認証を行った後、認証領域52へのアクセスを要求するコマンドを送信する。制御コマンド処理部24は、そのコマンドを解釈し、認証に成功している場合、アクセス制御部25に大容量不揮発性メモリ50へのアクセス制御を指示し、R/W装置69からデータI/F部21を通じて送られたデータが認証領域52に書き込まれ、また、認証領域52から読み出されたデータがデータI/F部21を介してR/W装置69に送信される。

【0019】

また、セキュア領域51へのデータの書き込み・読み出しを要求するR/W装置69のコマンドは、それを解釈した制御コマンド処理部24の指示で、アクセス制御部25からIC部11に転送される。IC部11のICコマンド処理部13は、このコマンドを解釈し、認証を要求しているときは、IC認証部15にR/W装置69の認証処理を行わせ、コマンドがセキュア領域51へのデータの書き込み・読み出しを要求しているときは、IC認証部15の認証処理が済んでいるのを確認した後、メモリ管理部16にセキュア領域

51へのデータの書き込み・読み出しを指示する。指示を受けたメモリ管理部16は、R/W装置69からアクセス制御部25を通じてIC部11に送られたデータを暗復号回路17で暗号化し、大容量不揮発性メモリI/F部26を介して、大容量不揮発性メモリ50のセキュア領域51に書き込む。また、セキュア領域51から読み出したデータは、暗復号回路17で復号化してICコマンド処理部13に送る。このデータは、制御部20のデータI/F部21からR/W装置69に送信される。

【0020】

このように、このセキュアメモリカード10では、非認証領域53よりも認証領域52の方がセキュリティレベルは高く、認証領域52よりもセキュア領域51の方がセキュリティレベルは高い。セキュア領域51は、秘匿性が高いアプリケーションや、ICカードに搭載されたアプリケーションが扱う大容量データを格納する場として適しており、認証領域52は、著作権が保護されたコンテンツを蓄積するのに適している。また、秘匿の必要が無い一般的なデータや解読される虞が無い暗号化されたデータであれば、非認証領域53に格納しても良い。そのため、秘匿性が高いアプリケーションを多く蓄積しようとするユーザは、セキュア領域51が広いことを望み、著作権が保護されたコンテンツを多く蓄積するユーザは、広い認証領域52を希望し、秘匿の必要が無い一般的なデータを専ら格納するユーザは、非認証領域53の拡大を希望する。

【0021】

セキュアメモリカードの認証領域、非認証領域及びセキュア領域の大きさが、こうしたユーザの意向に基づいて設定できるようにするため、本発明の実施形態のセキュアメモリカードは、図1に示すように、メモリ領域78の再分割を要求する外部からの分割要求コマンドを受信し、処理結果を外部に送信するコマンド送受信手段73と、メモリ領域78の更新条件を管理する領域更新条件管理手段71と、メモリ領域78の分割要求が領域更新条件管理手段71で管理する領域更新条件を満足するか否かを判断する領域更新判断手段72と、領域分割要求が領域更新条件を満たしているとき、メモリ領域78を再フォーマットする領域更新手段77と、メモリ領域78のアドレス等を管理する領域管理手段76と、メモリ領域78の初期分割や、分割された領域への初期値データの格納を行う初期化手段75と、分割要求に基づいてメモリ領域78の再分割が正常に行われたことを示すレシートを作成するレシート作成手段74とを備えている。

また、領域更新手段77は、それぞれのセキュリティレベルのメモリ分割領域を設定する領域更新手段771～774を備えており、その内の幾つかの領域更新手段によってメモリ領域78に設定されたセキュリティレベルの異なるメモリ分割領域を、ここでは領域1(781)～領域a(783)として表している。

【0022】

このセキュアメモリカード70のメモリ領域78は、図7の大容量不揮発性メモリ50に相当し、領域1(781)～領域a(783)は、図7の非認証領域53、認証領域52、セキュア領域51などに対応している。また、領域管理手段76は、図7の大容量不揮発性メモリ50のアドレス情報管理領域54を管理する手段であり、この領域管理手段76を始めとして、コマンド送受信手段73、領域更新条件管理手段71、領域更新判断手段72、領域更新手段77、初期化手段75及びレシート作成手段74は、図7の制御部20に設けられる。

【0023】

領域更新条件管理手段71は、図2に示すように、領域更新条件を規定したテーブルを管理している。領域更新条件は、手続きを規定する手続条件(図2(a))と、領域更新の実体を規定する実体条件(図2(b))とから成り、手続条件では、領域分割を行う時期(タイミング)に対応付けて、認証の必要性、及び、コマンドの暗号化の必要性が規定され、また、実体条件では、分割可能回数、メモリ領域78の最大分割数、1つのメモリ分割領域当たりの最大サイズ等が規定されている。なお、この手続条件や実体条件は、カード発行者、サービス運用者などが様々な理由で決め得るものであり、手続条件については、カードの交付前後で区別しない場合も当然有り得る。

【0024】

出荷段階のセキュアメモリカード70のメモリ領域78には、予め決められた大きさの非認証領域、認証領域及びセキュア領域が、初期化手段75によって設定され、それぞれのメモリ分割領域には、初期データが初期化手段75によって書き込まれている。

領域管理手段76は、このメモリ領域78におけるメモリ分割領域のアドレス情報を管理している。図3は、領域管理手段76が管理する領域管理情報を例示している。ここでは、メモリ分割領域のセキュリティレベルを示す領域識別子と、そのメモリ分割領域のメモリ領域78上の位置を示すアドレス値と、そのメモリ分割領域の中で実データが格納されている範囲を示すアドレス値とが管理されている。

【0025】

このセキュアメモリカード70をユーザが店頭で購入するとき、セキュアメモリカード70は、店頭のR/W装置にセットされ、R/W装置の操作を通じて、メモリ領域78にユーザの希望する大きさのメモリ分割領域が設定される。

図4のフロー図は、領域分割が行われるセキュアメモリカード70内の処理手順を示している。この処理に先立ち、R/W装置及びセキュアメモリカード70は、相互認証を実行し、また、領域更新条件の手続条件（図2（a））で規定されたカード発行者との外部認証を実行する。

【0026】

なお、カード内では、一般的にカードの状態遷移（カード用語で「ライフサイクル」と言う）を管理しており、ユーザパスワードが設定された瞬間にライフサイクルは「交付済みモード」となる。ユーザパスワードが設定されていない現段階では、ライフサイクルは「交付前モード」であり、そのため「交付前」の手続条件で規定された処理を実行することになる。

また、カード内において分割処理要求の受信状況をフラグで管理し、このフラグを参照して処理を決定するようにしても良い。この場合、フラグ初期値として「A（交付前モード）」を設定し、最初の分割処理要求を受信するとAモードにて処理を行い、この処理が完了するとフラグ値を「B（交付後モード）」に設定し、それ以降の分割処理要求はBモードにて処理する。現段階でのフラグは、初期値の「A（交付前モード）」であり、そのため「交付前」の手続条件で規定された処理を実行することになる。

【0027】

コマンド送受信手段73がR/W装置からメモリ分割領域の数やサイズ、属性等の情報を含む分割要求コマンドを受信すると、領域更新判断手段72は、そのメモリ分割領域の数やサイズ、属性等の情報を取得し（ステップ1）、その分割要求が領域更新条件管理手段71で管理されている領域更新条件の実体条件（図2（b））を満たしているか否かを判定する（ステップ2）。

領域更新判断手段72は、分割要求が領域更新条件を満たす場合に、図5のように、その分割要求に関する事項を記録して永続的または一時的に保持し、「今回の分割する領域サイズ」の情報を領域更新手段77に伝えてメモリ領域78の更新を依頼する。領域更新手段77は、領域管理手段76が管理するメモリ領域78の領域管理情報から、実データが格納されていない未使用領域を求め、この未使用領域を再フォーマットして、依頼されたサイズのメモリ分割領域を、該当するセキュリティレベルの領域更新手段771～774を用いて設定する（ステップ3）。

【0028】

初期化手段75は、更新されたメモリ分割領域に、必要な初期データ（あるいは更新データ）を格納する（ステップ4）。これらの処理に伴い、領域管理手段76は、管理する領域管理情報を更新する。

レシート作成手段74は、セキュアメモリカード70の識別情報や更新後のメモリ分割領域のサイズ、あるいは、更新前後におけるメモリ分割領域の差分サイズ等の情報を含むレシートを作成する（ステップ5）。このレシートは、コマンド送受信手段73からR/W装置に出力され、R/W装置の画面等に表示される。

このセキュアメモリカード70は、ユーザのパスワードが書き込まれた後、ユーザに交付される。

図6には、更新前のメモリ分割領域(図6(a))と、ユーザの意向に従って再フォーマットされた更新後のメモリ分割領域(図6(b)、(c)、(d))とを模式的に示している。

【0029】

このように、このセキュアメモリカードは、ユーザに交付する際に、メモリ領域をユーザの意向に基づいて分割することができる。そのため、ユーザは、既成のものではなく、オリジナルのカードを店頭で入手することができる。一方、カードメーカーは、顧客の要求に応えるために、メモリ分割領域の数や大きさを色々変えた各種のモデルを予め用意する必要がなくなる。従って、特定モデルの過剰在庫を回避することができる。

【0030】

なお、ここでは、セキュアメモリカードをR/W装置に装着し、このR/W装置を操作して、メモリ領域の分割要求コマンドをセキュアメモリカードに出力する場合について説明したが、セキュアメモリカードに予め幾つかの領域分割のパターン情報を格納し、その中から、セキュアメモリカードで実施すべき領域分割のパターンを、R/W装置を用いて選択するようにしてもよい。

【0031】

また、セキュアメモリカードのメモリ領域の再フォーマットは、交付されたカードを使用中のユーザが、メモリ分割領域の変更を必要とするときにも受けることができる。

この場合、ユーザが持参したセキュアメモリカードを店頭のR/W装置に装着してメモリ領域の再フォーマットが行われる。R/W装置及びセキュアメモリカードは、相互認証を実行し、また、領域更新条件の手続条件(図2(a))で規定されたカード発行者との外部認証や所有者のパスワード照合を行う。次いで、セキュアメモリカード内で図4の処理が行われ、実データの格納されていない未使用領域が再フォーマットされる。

あるいは、この場合、再フォーマット前のメモリ領域に格納されているデータを一旦R/W装置に退避し、メモリ領域を分割要求に従って再フォーマットした後、退避したデータを更新後のメモリ分割領域に書き戻すようにしても良い。

【0032】

このように、交付後のセキュアメモリカードのメモリ分割領域を再フォーマットすることが可能であるため、ユーザは、嗜好や社会トレンドが変わったときに、セキュアメモリカードを買い替えずに、カードの再フォーマット化で対処することができる。一方、カードメーカーは、発行済みのカードを保有するユーザと接する機会が生じるため、それを機にユーザへのサービス拡大を図ることが可能になる。

【0033】

また、このセキュアメモリカードは、メモリ領域に施された領域分割が、ユーザのパスワードの登録によって実効性を持つように構成することができる。この場合、セキュアメモリカードには、領域更新手段が実行したメモリ分割領域の更新に関する情報を出力する出力手段(レシート作成手段74)と、前記情報に対するユーザの確認登録を受け付ける受付手段とを設け、メモリ分割領域の更新は、確認登録の受け付けにより始めて実効性を持つように構成する。ユーザは、カードメーカーに事前にセキュアメモリカードの領域分割要求を伝え、この要求に従ってフォーマットされたセキュアメモリカードを店頭等で受け取るときに、レシート作成手段74が作成したレシートで領域分割を確認し、セキュアメモリカードにパスワードを登録する。この登録により、セキュアメモリカードの使用が可能になる。

こうした運用は、特別仕様の領域分割を施したカードを大量発注するような場合に極めて有利であり、領域分割要求を事前連絡することにより、店頭等で待たずにカードを受け取ることができる。また、パスワードが未登録のセキュアメモリカードを通信販売等のルートで頒布し、これを入手したユーザが端末からパスワードを登録してカードを使用可能にする、といった運用も可能である。

【0034】

なお、カードのメモリ分割領域を更新するR/W装置は、店頭の専用固定端末であっても、それ以外の携帯端末（携帯電話・PDAなど）であっても構わない。また、メモリ分割領域が更新されるカードは、携帯端末などに着脱可能に装着されるものであっても、携帯端末などに埋め込まれるチップ形態のものであっても良い。

【産業上の利用可能性】

【0035】

本発明は、半導体メモリカードやICカード、セキュアメモリカード、セキュアデバイス等と称される各種の情報記録装置に適用して、これらの情報記憶装置におけるメモリ領域のフォーマットにユーザの意思を反映させることができる。

【図面の簡単な説明】

【0036】

- 【図1】 本発明の実施形態におけるセキュアメモリカードの構成を示すブロック図
- 【図2】 本発明の実施形態におけるセキュアメモリカードの領域更新条件を示す図
- 【図3】 本発明の実施形態におけるセキュアメモリカードの領域管理情報を示す図
- 【図4】 本発明の実施形態におけるセキュアメモリカードの動作を示すフロー図
- 【図5】 本発明の実施形態におけるセキュアメモリカードの領域更新判断手段が保持する情報を示す図
- 【図6】 (a) 更新前のメモリ分割領域を模式的に示す図 (b) 更新後のメモリ分割領域を模式的に示す図
- 【図7】 セキュアメモリカードの構成を示すブロック図
- 【図8】 従来の半導体メモリカードの構成を示すブロック図

【符号の説明】

【0037】

- 10 セキュアメモリカード
- 11 IC部
- 12 I/F部
- 13 ICコマンド処理部
- 14 ファイル管理部
- 15 IC認証部
- 16 メモリ管理部
- 17 暗復号回路
- 18 内部不揮発性メモリ I/F部
- 20 制御部
- 21 データ I/F部
- 22 コマンド I/F部
- 23 制御認証部
- 24 コマンド処理部
- 25 アクセス制御部
- 26 大容量不揮発性メモリ I/F部
- 41 内部不揮発性メモリ
- 50 大容量不揮発性メモリ
- 51 セキュア領域
- 52 認証領域
- 53 非認証領域
- 54 アドレス情報管理領域
- 69 R/W装置
- 71 領域更新条件管理手段
- 72 領域更新判断手段
- 73 コマンド送受信手段

7 4 レシート作成手段
7 5 初期化手段
7 6 領域管理手段
7 7 領域更新手段
7 8 メモリ領域
1 0 9 メモリカード
3 0 2 コントロール I C
3 0 3 フラッシュメモリ
3 2 1 認証部
3 2 2 コマンド判定制御部
3 2 5 認証領域アクセス制御部
3 2 6 非認証領域アクセス制御
3 3 1 非認証領域
3 3 2 認証領域
7 7 1 レベル 1 領域更新手段
7 7 2 レベル 2 領域更新手段
7 7 3 レベル 3 領域更新手段
7 7 4 レベル n 領域更新手段
7 8 1 領域 1
7 8 2 領域 2
7 8 3 領域 a

【図 2】

タイミング	認証の有無	暗号化の必要性
交付前	カード発行者との外部認証	なし
交付後	カード発行者との外部認証 所有者のパスワード照合	あり
...

(a)

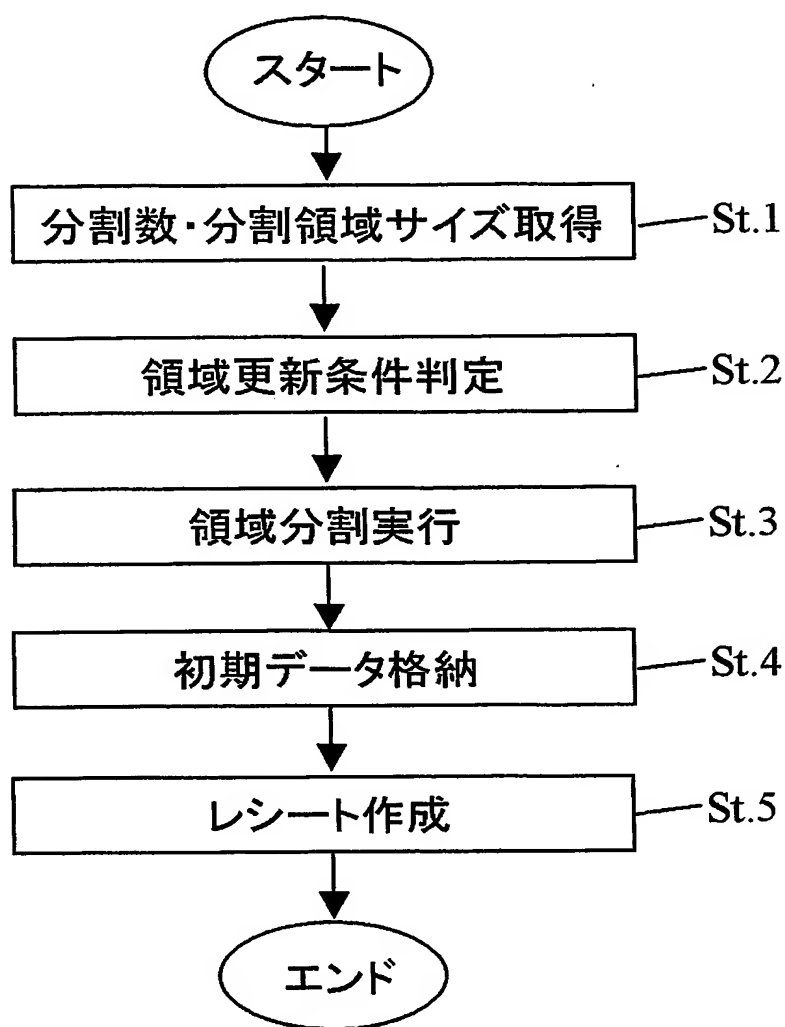
分割可能回数	3回
最大領域分割数	3
1領域あたりの最大サイズ	△バイト
...	...

(b)

【図3】

領域識別子	配置場所	実データを保持している場所
レベル1	アドレスa~b	アドレスa~a'
レベル2	アドレスc~d	アドレスc~c'

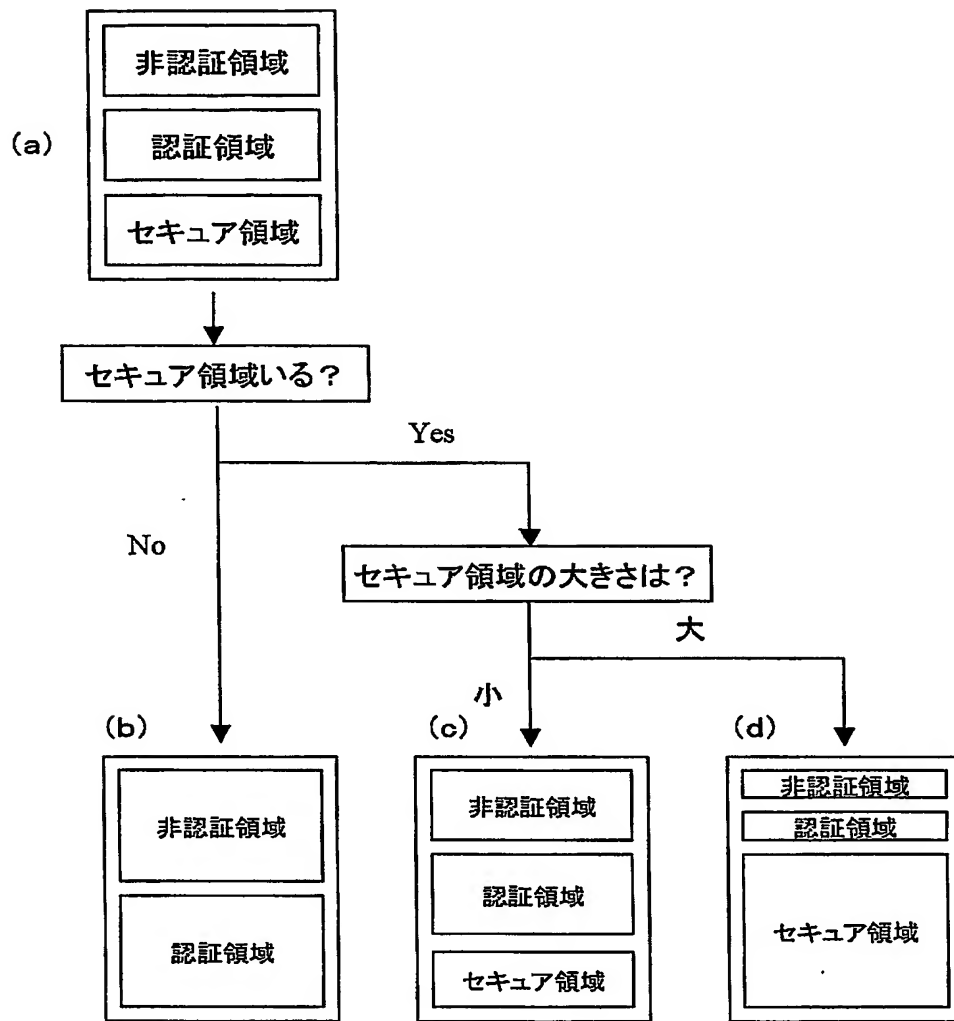
【図 4】



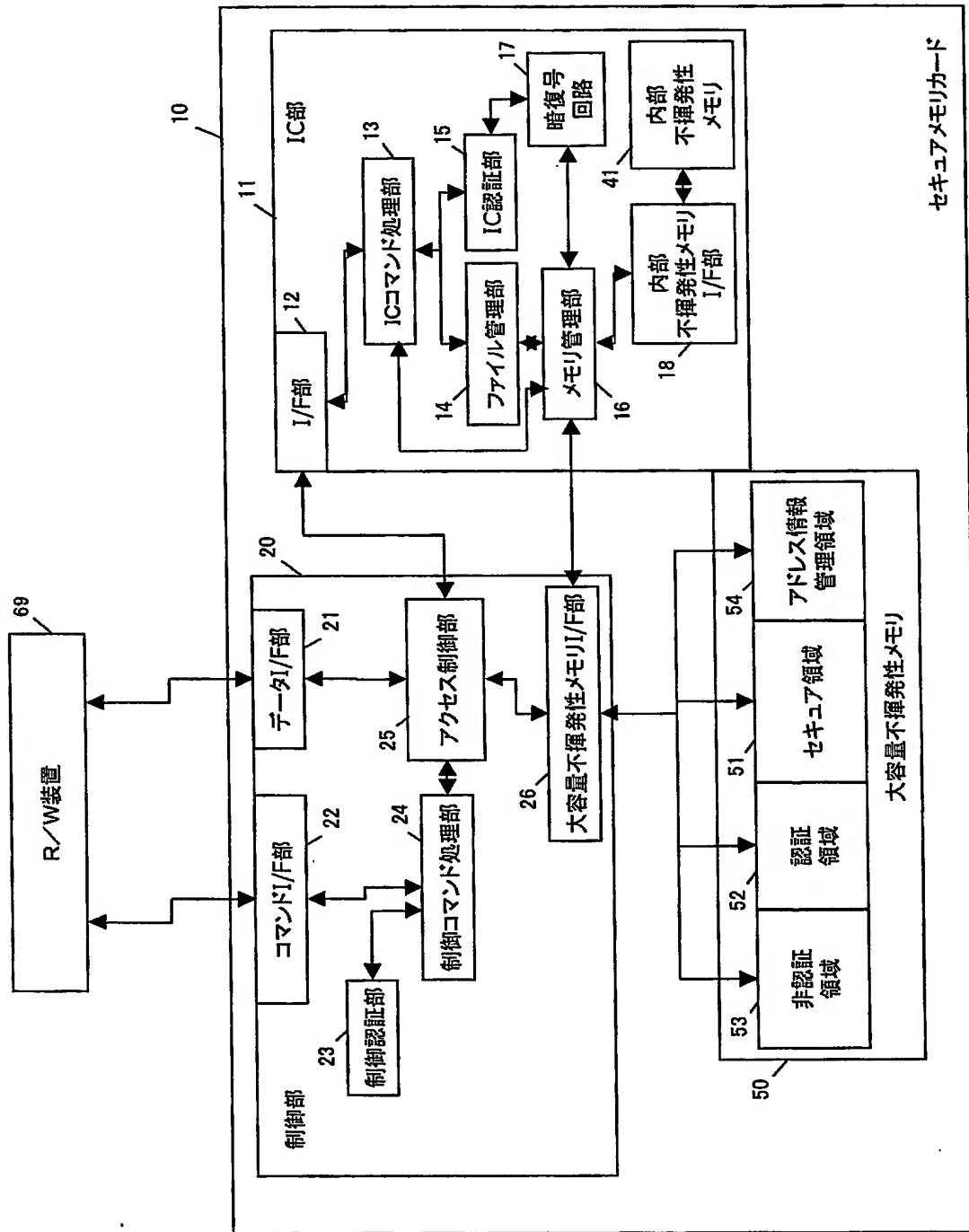
【図 5】

項目	内容
タイミング	交付後
認証相手	カード発行者
暗号化の有無	無
分割を実施した回数	一回
今回の分割する領域サイズ	レベル1：aバイト、レベル2：b バイト
...	...

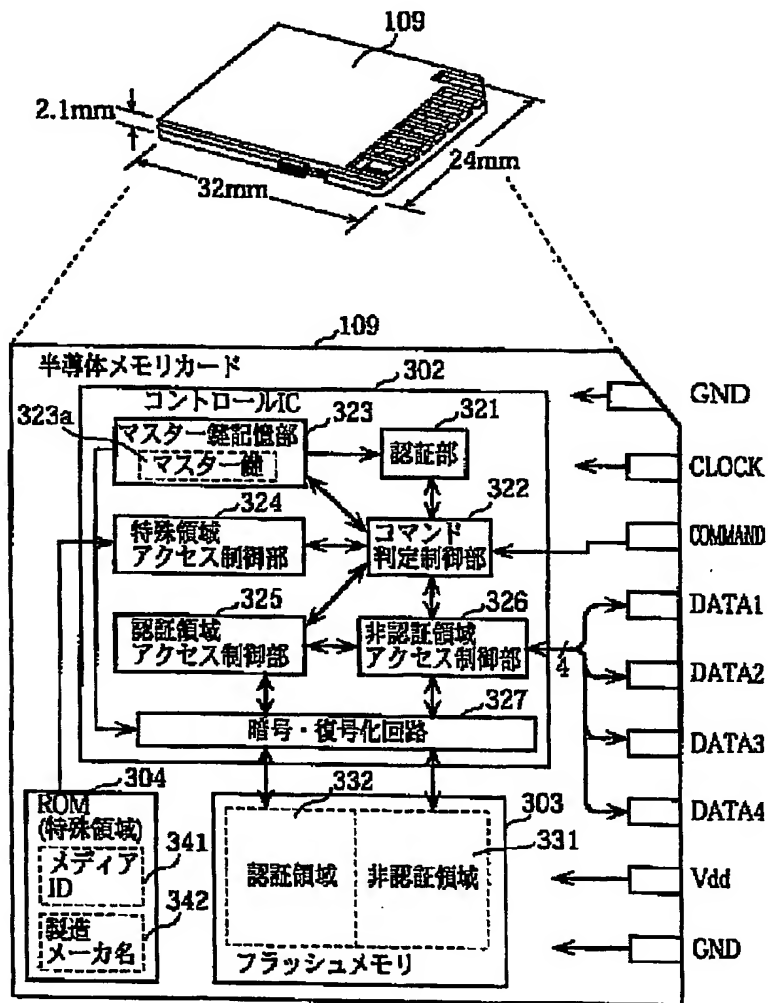
【図 6】



【図7】



【図 8】



【書類名】 要約書**【要約】**

【課題】 メモリ領域を分割する分割領域の数や大きさを、ユーザの意向に基づいて設定することができる情報記憶装置を提供する。

【解決手段】 メモリ領域 78 内にセキュリティレベルが異なる複数の分割領域 781 ～ 783 を有する情報記憶装置 70 に、分割領域のメモリ領域内でのアドレスを管理する領域管理手段 76 と、分割領域の数または大きさを更新する際の更新条件を管理する領域更新条件管理手段 71 と、分割領域の数または大きさの更新を要求する分割要求が更新条件を満足するか否かを判断する領域更新判断手段 72 と、分割要求が更新条件を満足するとき、分割要求に従ってメモリ領域内の分割領域の更新を実行する領域更新手段 77 とを設ける。この情報記憶装置 70 は、ユーザの意向を反映した分割要求により、メモリ領域 78 内の分割領域 781 ～ 783 がユーザの意図するように更新される。

【選択図】 図 1

特願 2 0 0 3 - 2 8 8 7 9 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社